III. REMARKS

Claims 1-15 are pending in this application. By the amendment, claims 6 and 13-15 have been amended. These amendments and remarks are being made to facilitate early allowance of the presently claimed subject matter. Applicants do not acquiesce in the correctness of the rejections and reserve the right to present specific arguments regarding any rejected claims not specifically addressed. Further, Applicants reserve the right to pursue the full scope of the subject matter of the original claims in a subsequent patent application that claims priority to the instant application. Reconsideration in view of the above amendments and following remarks is respectfully requested.

Claims 6, 13 and 14 have been revised to correct minor typographical errors. Applicants submit that those revisions do not affect the patentability of the claimed invention.

In the Office Action, claims 1-15 are rejected under 35 U.S.C. §103(a) over Riggins et al. (International Publication Number WO00/11832). This rejection is respectfully traversed, for the reasons that follow:

1. There is no motivation or suggestion to modify Riggins et al. as indicated by the Office

Applicants submit that there is no motivation or suggestion to modify Riggins et al. as indicated by the Office. Specifically, as conceded by the Office, Riggins et al. fail to disclose or suggest features such as, *inter alia*, a security policy as claimed in claims 1 and 15 and method of routing all incoming requests as claimed in claim 7. Applicants respectfully submit that incorporation of such features in Riggins et al. is neither motivated, suggested, nor even desirable. Riggins et al. disclose a firewall system, which controls the access to a computer network. *See e.g.*, Title and Abstract. The firewall system of Riggins et al. first authenticates a user based on a user identification. *See e.g.*, page 7, lines 1-7. After authentication, a user can access certain services provided by the server that are predetermined to be accessible by this particular user. *See e.g.*, page 9, line 25- page 10, line 2. Thus, the Riggins et al. system is a simple identification authenticating firewall system in which the services that a particular user (identified to the system) can access are predetermined. As such, there is no need to further check of the security status of a user, and a person with ordinary skill in the art would have no motivation to modify Riggins et al. to incorporate a security policy. Rather, the addition of a security policy would change and unnecessarily complicate the core principle of the operation of the system of Riggins et al. (i.e., to simplify the authentication process). *See e.g.*, page 7, lines 8-24 ("[T]he user need only maintain the URL of the global server 106, and identification and authentication information such as a password or hardware token for obtaining access to the functionality of the global server 106").

In addition, because the Riggins et al. system only checks identification of a user, "routing all incoming requests created by this [user]," which is claimed in the present invention, is not necessary in Riggins et al. Routing under the present invention has the function of, *inter alia*, converting device specific requests to a canonical form. In sharp contrast, in Riggins et al., all the requests for authentication are in the same form, i.e., identification of a user. *See e.g.*, page 7, lines 8-24. Thus, adding the feature of routing all incoming requests of the claimed invention to the system of Riggins et al. would only further complicate that system and reduce its' overall efficiency.

The undesirability of incorporating the security policy and routing feature of the claimed invention within the Riggins et al. system is predicated by the difference in principles between the Riggins et al. system and the present invention. For example, under the system of the claimed invention, one or more clients communicate with a server by means of requests for accessing an application function. The system chooses and executes an authentication mechanism based on the information contained in the client request, resulting in a security state. Thereafter, the system compares the security state to a security policy to see whether the security state of the clients fulfills the security level required for the specific request. *See e.g.*, claim 1 of the present invention. In contrast, under Riggins et al., the system predetermines the services that a specific client might access. When a client accesses the system through the authentication of identification by the firewall, it will choose services (application functions) from among the services the client is permitted to access. In view of these differences, Applicants respectfully submit that there is no motivation to modify Riggins et al. as indicated in the Office Action..

In view of the foregoing, Applicants respectfully request withdrawal of the rejections.

2. Riggins et al., even if modified with the hindsight of the present invention, still fail to disclose or suggest each and every claimed feature of the current invention

With regard to claims 1, 7 and 15, Applicants respectfully submit that even if the system of Riggins et al. is modified as indicated by the Office, Riggins et al. still fail to disclose or suggest each and every feature of the claimed invention. For example, Riggins et al. fail to disclose or suggest that "one or more clients communicate with said server by means of requests for accessing one of said application functions[,]" as recited in claim 1, 7 and 15. In contrast, in

Riggins et al, a client does not communicate with the system by means of requests for accessing one of the services, instead, a client will first be authenticated and then access its predetermined functionality. The only communication with the system in Riggins et al. is the identification information of the client, not the request for one of the services (functionality) of the server. *See generally* page 7, lines 1-24. In Riggins et al., various predetermined levels of access are granted to the client. However, in the authentication process, the client does not communicate with the system about the level of access. *See Id*; *See also* page 9, line 25- page 10, line 2.

In addition, Riggins et al. fail to disclose or suggest, *inter alia*, a system "containing a plurality of authentication mechanisms, and selecting and executing an authentication mechanism from said plurality of authentication mechanisms based on the information contained in the client request[,]" as recited in claim 1, 7 and 15. Rather, there is no disclosure, suggestion, or even hint in Riggins et al. about multiple authentication mechanisms and the selection of an authentication mechanism therefrom based on information in requests.

In view of the foregoing, even if Riggins et al. is modified to incorporate a "security policy" and "routing," *arguendo*, as the Office has alleged, Riggins et al. still fails to disclose or suggest each and every feature of the claimed invention. Accordingly, Applicants request withdrawal of the rejections.

Claims 2-6 are dependent upon claim 1 and claims 8-14 are dependent upon claim 7. The dependent claims are believed to be allowable based on the above arguments, as well as for their own additional features.

Applicants respectfully submit that the application is in condition for allowance. Should the Examiner believe that anything further is necessary to place the application in better condition for allowance, he is requested to contact Applicants' undersigned attorney at the telephone number listed below.

Respectfully submitted,

Ronald A. D'Alessandro
Reg. No.: 42,456

Date: 6/23/04

Hoffman, Warnick & D'Alessandro LLC
Three E-Comm Square
Albany, New York 12207
Telephone (518) 449-0044
Facsimile (518) 449-0047